

## Professional Cloud Network Engineer

Passing Score: 800

Time Limit: 120 min

File Version: 1

Professional Cloud Network Engineer



**Website:** <https://vceplus.com>

**VCE to PDF Converter:** <https://vceplus.com/vce-to-pdf/>

**Facebook:** <https://www.facebook.com/VCE.For.All.VN/>

**Twitter :** [https://twitter.com/VCE\\_Plus](https://twitter.com/VCE_Plus)

<https://vceplus.com/>

## Exam A

### QUESTION 1

Your organization is deploying a single project for 3 separate departments. Two of these departments require network connectivity between each other, but the third department should remain in isolation. Your design should create separate network administrative domains between these departments. You want to minimize operational overhead.



<https://vceplus.com/> How should

you design the topology?

- A. Create a Shared VPC Host Project and the respective Service Projects for each of the 3 separate departments.
- B. Create 3 separate VPCs, and use Cloud VPN to establish connectivity between the two appropriate VPCs.
- C. Create 3 separate VPCs, and use VPC peering to establish connectivity between the two appropriate VPCs.
- D. Create a single project, and deploy specific firewall rules. Use network tags to isolate access between the departments.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Use Shared VPC to connect to a common VPC network. Resources in those projects can communicate with each other securely and efficiently across project boundaries using internal IPs. You can manage shared network resources, such as subnets, routes, and firewalls, from a central host project, enabling you to apply and enforce consistent network policies across the projects.

With Shared VPC and IAM controls, you can separate network administration from project administration. This separation helps you implement the principle of least privilege. For example, a centralized network team can administer the network without having any permissions into the participating projects. Similarly, the project admins can manage their project resources without any permissions to manipulate the shared network.

Reference: <https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations>

## QUESTION 2

You are using a third-party next-generation firewall to inspect traffic. You created a custom route of 0.0.0.0/0 to route egress traffic to the firewall. You want to allow your VPC instances without public IP addresses to access the BigQuery and Cloud Pub/Sub APIs, without sending the traffic through the firewall.

Which two actions should you take? (Choose two.)

- A. Turn on Private Google Access at the subnet level.
- B. Turn on Private Google Access at the VPC level.
- C. Turn on Private Services Access at the VPC level.
- D. Create a set of custom static routes to send traffic to the external IP addresses of Google APIs and services via the default internet gateway.
- E. Create a set of custom static routes to send traffic to the internal IP addresses of Google APIs and services via the default internet gateway.

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://cloud.google.com/vpc/docs/private-access-options>

## QUESTION 3

All the instances in your project are configured with the custom metadata `enable-oslogin` value set to FALSE and to block project-wide SSH keys. None of the instances are set with any SSH key, and no project-wide SSH keys have been configured. Firewall rules are set up to allow SSH sessions from any IP address range. You want to SSH into one instance.

What should you do?

- A. Open the Cloud Shell SSH into the instance using `gcloud compute ssh`.
- B. Set the custom metadata `enable-oslogin` to TRUE, and SSH into the instance using a third-party tool like putty or ssh.
- C. Generate a new SSH key pair. Verify the format of the private key and add it to the instance. SSH into the instance using a third-party tool like putty or ssh.
- D. Generate a new SSH key pair. Verify the format of the public key and add it to the project. SSH into the instance using a third-party tool like putty or ssh.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://cloud.google.com/compute/docs/storing-retrieving-metadata>

#### QUESTION 4

You work for a university that is migrating to GCP.

These are the cloud requirements:

- On-premises connectivity with 10 Gbps
- Lowest latency access to the cloud
- Centralized Networking Administration Team

New departments are asking for on-premises connectivity to their projects. You want to deploy the most cost-efficient interconnect solution for connecting the campus to Google Cloud.

What should you do?

- A. Use Shared VPC, and deploy the VLAN attachments and Interconnect in the host project.
- B. Use Shared VPC, and deploy the VLAN attachments in the service projects. Connect the VLAN attachment to the Shared VPC's host project.
- C. Use standalone projects, and deploy the VLAN attachments in the individual projects. Connect the VLAN attachment to the standalone projects' Interconnects.
- D. Use standalone projects and deploy the VLAN attachments and Interconnects in each of the individual projects.

**Correct Answer:** A

**Section:** (none)

**Explanation**



**Explanation/Reference:**

#### QUESTION 5

You have deployed a new internal application that provides HTTP and TFTP services to on-premises hosts. You want to be able to distribute traffic across multiple Compute Engine instances, but need to ensure that clients are sticky to a particular instance across both services.

Which session affinity should you choose?

- A. None
- B. Client IP
- C. Client IP and protocol
- D. Client IP, port and protocol

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

### QUESTION 6

You want to deploy a VPN Gateway to connect your on-premises network to GCP. You are using a non BGP-capable on-premises VPN device. You want to minimize downtime and operational overhead when your network grows. The device supports only IKEv2, and you want to follow Google-recommended practices.

What should you do?

- A.
  - Create a Cloud VPN instance.
  - Create a policy-based VPN tunnel per subnet.
  - Configure the appropriate local and remote traffic selectors to match your local and remote networks.
  - Create the appropriate static routes.
- B.
  - Create a Cloud VPN instance.
  - Create a policy-based VPN tunnel.
  - Configure the appropriate local and remote traffic selectors to match your local and remote networks.
  - Configure the appropriate static routes.
- C.
  - Create a Cloud VPN instance.
  - Create a route-based VPN tunnel.
  - Configure the appropriate local and remote traffic selectors to match your local and remote networks.
  - Configure the appropriate static routes.
- D.
  - Create a Cloud VPN instance.
  - Create a route-based VPN tunnel.
  - Configure the appropriate local and remote traffic selectors to 0.0.0.0/0.
  - Configure the appropriate static routes.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing>

### QUESTION 7

Your company just completed the acquisition of Altostrat (a current GCP customer). Each company has a separate organization in GCP and has implemented a custom DNS solution. Each organization will retain its current domain and host names until after a full transition and architectural review is done in one year. These are the assumptions for both GCP environments.

- Each organization has enabled full connectivity between all of its projects by using Shared VPC.
- Both organizations strictly use the 10.0.0.0/8 address space for their instances, except for bastion hosts (for accessing the instances) and load balancers for serving web traffic.
- There are no prefix overlaps between the two organizations.
- Both organizations already have firewall rules that allow all inbound and outbound traffic from the 10.0.0.0/8 address space.
- Neither organization has Interconnects to their on-premises environment.

You want to integrate networking and DNS infrastructure of both organizations as quickly as possible and with minimal downtime.

Which two steps should you take? (Choose two.)

- A. Provision Cloud Interconnect to connect both organizations together.
- B. Set up some variant of DNS forwarding and zone transfers in each organization.
- C. Connect VPCs in both organizations using Cloud VPN together with Cloud Router.
- D. Use Cloud DNS to create A records of all VMs and resources across all projects in both organizations.
- E. Create a third organization with a new host project, and attach all projects from your company and Altostrat to it using shared VPC.

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 8

Your on-premises data center has 2 routers connected to your Google Cloud environment through a VPN on each router. All applications are working correctly; however, all of the traffic is passing across a single VPN instead of being load-balanced across the 2 connections as desired.

During troubleshooting you find:

- Each on-premises router is configured with a unique ASN.
- Each on-premises router is configured with the same routes and priorities.
- Both on-premises routers are configured with a VPN connected to a single Cloud Router.
- BGP sessions are established between both on-premises routers and the Cloud Router.
- Only 1 of the on-premises router's routes are being added to the routing table.

What is the most likely cause of this problem?

- A. The on-premises routers are configured with the same routes.
- B. A firewall is blocking the traffic across the second VPN connection.
- C. You do not have a load balancer to load-balance the network traffic.
- D. The ASNs being used on the on-premises routers are different.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 9

You have ordered Dedicated Interconnect in the GCP Console and need to give the Letter of Authorization/Connecting Facility Assignment (LOA-CFA) to your cross-connect provider to complete the physical connection.

Which two actions can accomplish this? (Choose two.)

- A. Open a Cloud Support ticket under the Cloud Interconnect category.
- B. Download the LOA-CFA from the Hybrid Connectivity section of the GCP Console.
- C. Run `gcloud compute interconnects describe <interconnect>`.
- D. Check the email for the account of the NOC contact that you specified during the ordering process.
- E. Contact your cross-connect provider and inform them that Google automatically sent the LOA/CFA to them via email, and to complete the connection.

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 10

Your company's web server administrator is migrating on-premises backend servers for an application to GCP. Libraries and configurations differ significantly across these backend servers. The migration to GCP will be lift-and-shift, and all requests to the servers will be served by a single network load balancer frontend. You want to use a GCP-native solution when possible.

How should you deploy this service in GCP?

- A. Create a managed instance group from one of the images of the on-premises servers, and link this instance group to a target pool behind your load balancer.
- B. Create a target pool, add all backend instances to this target pool, and deploy the target pool behind your load balancer.
- C. Deploy a third-party virtual appliance as frontend to these servers that will accommodate the significant differences between these backend servers.
- D. Use GCP's ECMP capability to load-balance traffic to the backend servers by installing multiple equal-priority static routes to the backend servers.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://cloud.google.com/compute/docs/instance-groups/adding-an-instance-group-to-a-load-balancer>

#### QUESTION 11

You want to set up two Cloud Routers so that one has an active Border Gateway Protocol (BGP) session, and the other one acts as a standby.

Which BGP attribute should you use on your on-premises router?

- A. AS-Path
- B. Community
- C. Local Preference
- D. Multi-exit Discriminator



**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://cloud.google.com/router/docs/concepts/overview>

#### QUESTION 12

You are increasing your usage of Cloud VPN between on-premises and GCP, and you want to support more traffic than a single tunnel can handle. You want to increase the available bandwidth using Cloud VPN.

What should you do?

- A. Double the MTU on your on-premises VPN gateway from 1460 bytes to 2920 bytes.
- B. Create two VPN tunnels on the same Cloud VPN gateway that point to the same destination VPN gateway IP address.



- C. Add a second on-premises VPN gateway with a different public IP address. Create a second tunnel on the existing Cloud VPN gateway that forwards the same IP range, but points at the new on-premises gateway IP.
- D. Add a second Cloud VPN gateway in a different region than the existing VPN gateway. Create a new tunnel on the second Cloud VPN gateway that forwards the same IP range, but points to the existing on-premises VPN gateway IP address.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 13

You converted an auto mode VPC network to custom mode. Since the conversion, some of your Cloud Deployment Manager templates are no longer working. You want to resolve the problem.

What should you do?

- A. Apply an additional IAM role to the Google API's service account to allow custom mode networks.
- B. Update the VPC firewall to allow the Cloud Deployment Manager to access the custom mode networks.
- C. Explicitly reference the custom mode networks in the Cloud Armor whitelist.
- D. Explicitly reference the custom mode networks in the Deployment Manager templates.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 14

You are using a 10-Gbps direct peering connection to Google together with the gsutil tool to upload files to Cloud Storage buckets from on-premises servers. The on-premises servers are 100 milliseconds away from the Google peering point. You notice that your uploads are not using the full 10-Gbps bandwidth available to you. You want to optimize the bandwidth utilization of the connection.

What should you do on your on-premises servers?

- A. Tune TCP parameters on the on-premises servers.



<https://vceplus.com/>

- B. Compress files using utilities like tar to reduce the size of data being sent.
- C. Remove the -m flag from the gsutil command to enable single-threaded transfers.
- D. Use the perfdiag parameter in your gsutil command to enable faster performance: `gsutil perfdiag gs://[BUCKET NAME].`

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 15

You work for a multinational enterprise that is moving to GCP.

These are the cloud requirements:

- An on-premises data center located in the United States in Oregon and New York with Dedicated Interconnects connected to Cloud regions us-west1 (primary HQ) and us-east4 (backup)
- Multiple regional offices in Europe and APAC
- Regional data processing is required in europe-west1 and australia-southeast1
- Centralized Network Administration Team

Your security and compliance team requires a virtual inline security appliance to perform L7 inspection for URL filtering. You want to deploy the appliance in uswest1.

What should you do?

- A.
  - Create 2 VPCs in a Shared VPC Host Project.
  - Configure a 2-NIC instance in zone us-west1-a in the Host Project.

- Attach NIC0 in VPC #1 us-west1 subnet of the Host Project.
  - Attach NIC1 in VPC #2 us-west1 subnet of the Host Project.
  - Deploy the instance.
  - Configure the necessary routes and firewall rules to pass traffic through the instance.
- B. • Create 2 VPCs in a Shared VPC Host Project.
- Configure a 2-NIC instance in zone us-west1-a in the Service Project.
  - Attach NIC0 in VPC #1 us-west1 subnet of the Host Project.
  - Attach NIC1 in VPC #2 us-west1 subnet of the Host Project.
  - Deploy the instance.
  - Configure the necessary routes and firewall rules to pass traffic through the instance.
- C. • Create 1 VPC in a Shared VPC Host Project.
- Configure a 2-NIC instance in zone us-west1-a in the Host Project.
  - Attach NIC0 in us-west1 subnet of the Host Project. • Attach NIC1 in us-west1 subnet of the Host Project
  - Deploy the instance.
  - Configure the necessary routes and firewall rules to pass traffic through the instance.
- D. • Create 1 VPC in a Shared VPC Service Project.
- Configure a 2-NIC instance in zone us-west1-a in the Service Project.
  - Attach NIC0 in us-west1 subnet of the Service Project.
  - Attach NIC1 in us-west1 subnet of the Service Project
  - Deploy the instance.
  - Configure the necessary routes and firewall rules to pass traffic through the instance.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 16

You are designing a Google Kubernetes Engine (GKE) cluster for your organization. The current cluster size is expected to host 10 nodes, with 20 Pods per node and 150 services. Because of the migration of new services over the next 2 years, there is a planned growth for 100 nodes, 200 Pods per node, and 1500 services. You want to use VPC-native clusters with alias IP ranges, while minimizing address consumption.

How should you design this topology?

- A. Create a subnet of size/25 with 2 secondary ranges of: /17 for Pods and /21 for Services. Create a VPC-native cluster and specify those ranges.

- B. Create a subnet of size/28 with 2 secondary ranges of: /24 for Pods and /24 for Services. Create a VPC-native cluster and specify those ranges. When the services are ready to be deployed, resize the subnets.
- C. Use `gcloud container clusters create [CLUSTER NAME] --enable-ip-alias` to create a VPC-native cluster.
- D. Use `gcloud container clusters create [CLUSTER NAME]` to create a VPC-native cluster.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters>

#### QUESTION 17

Your company is running out of network capacity to run a critical application in the on-premises data center. You want to migrate the application to GCP. You also want to ensure that the Security team does not lose their ability to monitor traffic to and from Compute Engine instances. Which two products should you incorporate into the solution? (Choose two.)

- A. VPC flow logs
- B. Firewall logs
- C. Cloud Audit logs
- D. Stackdriver Trace
- E. Compute Engine instance system logs



**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations>

#### QUESTION 18

You want to apply a new Cloud Armor policy to an application that is deployed in Google Kubernetes Engine (GKE). You want to find out which target to use for your Cloud Armor policy.

Which GKE resource should you use?

- A. GKE Node

- B. GKE Pod
- C. GKE Cluster
- D. GKE Ingress

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://cloud.google.com/kubernetes-engine/docs/how-to/cloud-armor-backendconfig>

#### QUESTION 19

You need to establish network connectivity between three Virtual Private Cloud networks, Sales, Marketing, and Finance, so that users can access resources in all three VPCs. You configure VPC peering between the Sales VPC and the Finance VPC. You also configure VPC peering between the Marketing VPC and the Finance VPC. After you complete the configuration, some users cannot connect to resources in the Sales VPC and the Marketing VPC. You want to resolve the problem.

What should you do?

- A. Configure VPC peering in a full mesh.
- B. Alter the routing table to resolve the asymmetric route.
- C. Create network tags to allow connectivity between all three VPCs.
- D. Delete the legacy network and recreate it to allow transitive peering.



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 20

You create multiple Compute Engine virtual machine instances to be used as TFTP servers.

Which type of load balancer should you use?

- A. HTTP(S) load balancer
- B. SSL proxy load balancer

- C. TCP proxy load balancer
- D. Network load balancer

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 21

You want to configure a NAT to perform address translation between your on-premises network blocks and GCP.

Which NAT solution should you use?

- A. Cloud NAT
- B. An instance with IP forwarding enabled
- C. An instance configured with iptables DNAT rules
- D. An instance configured with iptables SNAT rules

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://cloud.google.com/nat/docs/overview>

#### QUESTION 22

In order to provide subnet level isolation, you want to force instance-A in one subnet to route through a security appliance, called instance-B, in another subnet.

What should you do?

- A. Create a more specific route than the system-generated subnet route, pointing the next hop to instance-B with no tag.
- B. Create a more specific route than the system-generated subnet route, pointing the next hop to instance-B with a tag applied to instance-A.
- C. Delete the system-generated subnet route and create a specific route to instance-B with a tag applied to instance-A.
- D. Move instance-B to another VPC and, using multi-NIC, connect instance-B's interface to instance-A's network. Configure the appropriate routes to force traffic through to instance-A.

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

### QUESTION 23

Your company has a security team that manages firewalls and SSL certificates. It also has a networking team that manages the networking resources. The networking team needs to be able to read firewall rules, but should not be able to create, modify, or delete them.

How should you set up permissions for the networking team?

- A. Assign members of the networking team the compute.networkUser role.
- B. Assign members of the networking team the compute.networkAdmin role.
- C. Assign members of the networking team a custom role with only the compute.networks.\* and the compute.firewalls.list permissions.
- D. Assign members of the networking team the compute.networkViewer role, and add the compute.networks.use permission.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://cloud.google.com/compute/docs/access/iam>

### QUESTION 24

You have created an HTTP(S) load balanced service. You need to verify that your backend instances are responding properly.

How should you configure the health check?

- A. Set `request-path` to a specific URL used for health checking, and set `proxy-header` to `PROXY_V1`.
- B. Set `request-path` to a specific URL used for health checking, and set `host` to include a custom host header that identifies the health check.
- C. Set `request-path` to a specific URL used for health checking, and set `response` to a string that the backend service will always return in the response body.
- D. Set `proxy-header` to the default value, and set `host` to include a custom host header that identifies the health check.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://cloud.google.com/load-balancing/docs/health-checks>

**QUESTION 25**

You need to give each member of your network operations team least-privilege access to create, modify, and delete Cloud Interconnect VLAN attachments.

What should you do?

- A. Assign each user the editor role.
- B. Assign each user the compute.networkAdmin role.
- C. Give each user the following permissions only: compute.interconnectAttachments.create, compute.interconnectAttachments.get.
- D. Give each user the following permissions only: compute.interconnectAttachments.create, compute.interconnectAttachments.get, compute.routers.create, compute.routers.get, compute.routers.update.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



<https://vceplus.com/>